

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Taiji SASAGE, et al.

Application No.:

Group Art Unit:

Filed: January 29, 2002

Examiner:

For: METHOD FOR DETECTING AND MANAGING COMPUTER VIRUSES IN SYSTEM  
FOR SENDING OR RECEIVING ELECTRONIC MAIL

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN  
APPLICATION IN ACCORDANCE  
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s)  
herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2001-020404


Filed: January 29, 2001

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing  
date(s) as evidenced by the certified papers attached hereto, in accordance with the  
requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: January 29, 2002

By:   
H. J. Staas  
Registration No. 22,010

700 11th Street, N.W., Ste. 500  
Washington, D.C. 20001  
(202) 434-1500

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

Jc872 U.S.  
10/0578  
01/29/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日  
Date of Application: 2001年 1月29日

出 願 番 号  
Application Number: 特願2001-020404

[ST.10/C]: [JP2001-020404]

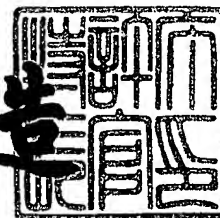
出 願 人  
Applicant(s): 富士通株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2002年 1月11日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3115112

【書類名】 特許願

【整理番号】 0000693

【提出日】 平成13年 1月29日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/06

【発明の名称】 メールウイルス検出用コンピュータ・プログラム

【請求項の数】 4

【発明者】

    【住所又は居所】 東京都大田区西蒲田7丁目37番10号 株式会社富士通アドバンスソリューションズ内

    【氏名】 捧 泰士

【発明者】

    【住所又は居所】 東京都大田区西蒲田 7丁目37番10号 株式会社富士通アドバンスソリューションズ内

    【氏名】 山岡 辰男

【特許出願人】

    【識別番号】 000005223

    【氏名又は名称】 富士通株式会社

【代理人】

    【識別番号】 100108187

    【弁理士】

    【氏名又は名称】 横山 淳一

    【電話番号】 044-754-3035

【手数料の表示】

    【予納台帳番号】 011280

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0017694

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 メールウイルス検出用コンピュータ・プログラム

【特許請求の範囲】

【請求項 1】 ネットワーク上を転送されるメールがメールウイルスに感染しているかいないかをチェックするメールウイルス検出用コンピュータ・プログラムであって、

コンピュータに、

前記ネットワーク上を転送されるメールで指定されているアドレスとしてメールウイルス検出用アドレスが指定されているかいないかを判定するアドレス判定手段と、

前記アドレス判定手段により、メールウイルス検出用アドレスが指定されていると判定されたメールと同型のメールの送信を抑止するメール抑止手段と、

を実現させるメールウイルス検出用コンピュータ・プログラム。

【請求項 2】 請求項 1 記載のコンピュータ・プログラムであって、

コンピュータに、

アドレス判定手段により検出されたメールに基づき必要連絡先に連絡を行うメールウイルス連絡手段

を実現させるメールウイルス検出用コンピュータ・プログラム。

【請求項 3】 ネットワーク上を転送されるメールがメールウイルスに感染しているかいないかをチェックするメールウイルス検出方法であって、

前記ネットワーク上を転送されるメールで指定されているアドレスとしてメールウイルス検出用アドレスが指定されているかいないかを判定するアドレス判定工程と、

前記アドレス判定工程により、メールウイルス検出用アドレスが指定されていると判定されたメールと同型のメールの送信を抑止するメール抑止工程を備えたことを特徴とするメールウイルス検出方法。

【請求項 4】 ネットワーク上を転送されるメールがメールウイルスに感染しているかいないかをチェックするメールウイルス検出用コンピュータ・プログラムを格納したコンピュータ読み取り可能な記録媒体であって、

コンピュータに、

前記ネットワーク上を転送されるメールで指定されているアドレスとしてメールウイルス検出用アドレスが指定されているかいないかを判定するアドレス判定工程と、

前記アドレス判定工程により、メールウイルス検出用アドレスが指定されていると判定されたメールと同型のメールの送信を抑止するメール抑止工程と

を実行させることを特徴とするメールウイルス検出用コンピュータ・プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、電子メールの送受信を行うメールシステムとコンピュータウイルスの検出、対応に関する。

【0002】

【従来の技術】

メールシステムあるいはメールシステムクライアントのコンピュータ環境において、既知のコンピュータウイルスに関する情報（例：パターンファイル）を備え、コンピュータ内のファイルやメールに添付されたデータとパターンファイルの内容とを対比することで、コンピュータウイルスを検出していた。その後メール送受信ログを調査する等して対応していた。

【0003】

【発明が解決しようとする課題】

しかしながら、従来の技術ではパターンファイルが対応しているコンピュータウイルスについてのみ、コンピュータウイルスの検出が可能であった。よって、未知のコンピュータウイルスを検出し何らかの対応がなされるのは、被害が拡大し、それが判明してからである。

【0004】

このコンピュータウイルスのうち、メールシステムクライアントのメールアドレス帳に登録してあるメールアドレス宛にコンピュータウイルス自身と同型のウ

ウイルスをメールとして送信するウイルス(以降メールウイルス)については、メール受信者のコンピュータが感染されるばかりでなく、メールアドレスにある他の人のコンピュータにまで感染する可能性があり、その場合、メール受信者がメールの発信者となるため、メール受信者までが加害者になりかねない。しかし、今までは被害者数を大きくしかねないこのような未知のメールウイルスに対しての対策がなかった。

#### 【0005】

このような未知のメールウイルスであっても早期に発見し、メールウイルスと思われるメールの送信を抑止し、メールウイルスの情報と発信者のメール送受信履歴を指定のメールアドレスに連絡することを課題とする。

#### 【0006】

##### 【課題を解決するための手段】

メールウイルス検出システムは、アドレス判定手段と、メール抑止手段、ウイルス連絡手段を備える。

#### 【0007】

アドレス判定手段は、メールアドレスが通常は送信される予定のないメールウイルス検出用アドレスへ送信されたものか否かを判定する。ウイルス連絡手段は、メールウイルス検出用アドレスへ送信があったことを示すメールアドレス検出を連絡する必要がある相手に、電子メールを送信する。メール抑止手段は、メールウイルス検出用アドレスへ送信されたメールと同型のメールの送信を抑止する。

#### 【0008】

本発明の利用方法は、使用者の存在しないメールアドレスをメール管理者が用意する。そのメールアドレスをウイルス検出用アドレスとしてメールシステムクライアントのアドレス帳に登録しておくこととするが、使用者の存在しないアドレスであるため、通常は送信されない。メールウイルスが多くの相手にウイルスを送信するのは、メールシステムクライアントのアドレス帳を利用するという特徴によるからである。しかし、本発明により、メールウイルスがLAN内に入ってきた場合に、メールウイルスがメールウイルス検出用アドレスに送信した時点で

メールウイルスを検出することができる。よって、それ以降、メールウイルスの可能性のあるメールの送信を自動的に抑止し、メールウイルスの情報、メール送受信ログを指定のメールアドレスに自動的に連絡することができるようになる。

【0009】

【発明の実施の形態】

図1は本発明のメールウイルス検出システムを適用してメールが転送されるネットワークの全体像の例を示す図である。

【0010】

メールウイルス検出システム101、メールシステムクライアント102、メール管理者のメールシステムクライアント103、およびインターネット上のメールシステム104がネットワーク105に接続されている。

【0011】

メールウイルス検出システム101は、メールプロトコルフロントエンドプログラム111、アドレス判定プログラム112、メール抑止プログラム113、メールウイルス連絡プログラム114、メールボックス115、メールウイルス情報テーブル116、メールウイルス用アドレステーブル117、抑止条件設定テーブル118、連絡レベルテーブル119、そしてメールウイルス連絡先テーブル120を有する。

【0012】

メールシステムクライアント102では、メールシステムを利用する前に、まずメールアドレス帳121にメールウイルス検出用だけに使用し、通常は使われる予定のないメールアドレスを登録しておく。この登録メールアドレスはメールウイルス用アドレステーブル117に登録されている値でなければならない。

【0013】

登録方法は、ここでは事前に決めてあるメールアドレスを手作業でメールシステムクライアント102のメールアドレス帳121に登録する方法にしているが、メールシステムクライアント102からメールウイルス検出システム101の問い合わせ用メールアドレスに問い合わせ、メールウイルス検出用アドレスを自動発行してもらう方式を作成・運用してもよい。



【0014】

その後、メールシステムクライアント102から送信されたメールは、メールプロトコルフロントエンドプログラム111により受信され、アドレス判定プログラム112によりメールウイルス用アドレスに宛てたメールか否かが比較判断される。それは通常ならばあり得ないので、すなわちメールウイルスに感染し、送信されたメールか否かが比較判断されることになる。

【0015】

メールウイルスに感染していなければ、すなわちメールの宛先とメールウイルス検出用アドレスが不一致であれば、メールはメールボックス115に記憶される。

同一ドメイン宛でない場合には、該当ドメインのメールシステムに転送する。

【0016】

メールがメールウイルス検出用アドレス宛であった、即ちメールウイルスに感染していたときは、アドレス判定プログラム112がウイルスに感染したメールを検出して、メール抑止プログラム113、メールウイルス連絡プログラム114にメールウイルス感染を検出したことを知らせる。

【0017】

メール抑止プログラム113はメールウイルスに感染したメールのサイズ、件名、送信者、日時を記憶し、以後同じ条件のメールの送信を抑止する。

【0018】

一方、メールウイルス連絡プログラム114は、メールウイルス検出後のメールウイルス連絡プログラム114によるメールとして該当するメールの送信元であるメールシステムクライアント102とメール管理者のメールシステムクライアント103宛てに自動的に送信する。

【0019】

メールシステムクライアント102およびメール管理者のメールシステムクライアント103は、そのメールウイルス検出を連絡するメールを受け取ることで、自分あるいはLAN内のメールによってメールウイルスに感染したことを知ることができるので、すぐに対策処理を行える。

## 【0020】

尚、メールウイルス検出システム101は、CPU／メモリ／外部記憶装置等を備えたコンピュータのOS（オペレーティングシステム）の制御の下でコンピュータ・プログラムが実行されることにより実現される。そしてメールウイルス検出システム101のプログラムは、フロッピーディスクやCD-ROMなどのリムーバブルな記録媒体もしくはネットワークを介して外部記憶装置に一旦格納され、メモリにロードされ実行される。

## 【0021】

図11は、LAN、インターネットで用いられるメールのヘッダー情報である。

## 【0022】

メールの「ヘッダー」には、メールの送信元メールアドレスである「from:」、送信先メールアドレスである「to:」、カーボンコピーの送信先メールアドレスである「cc:」、返信先メールアドレスである「reply-to:」、エラーメールの送信先メールアドレスである「return-path:」などがセットされている。

## 【0023】

よって、メールウイルスが検出された時は、メールの送信元メールアドレス、送信先メールアドレス、返信先メールアドレス等にメールウイルス検出の連絡を行うことが可能である。

## 【0024】

図2から図5は、本発明にかかわるメールウイルス検出システム101の動作の手順を示すフローチャートである。

## 【0025】

メールウイルス情報テーブル116の構成を図7に示す。メールウイルス情報テーブル116は、メールウイルスの概要を記録するものであり、「受信日時」、「送信者」、「サイズ」、「件名」、「連絡」の5項目で構成される。

## 【0026】

「受信日時」はメールウイルスに感染したメールを受信した日時である。「送

信者」は、そのメールの送信者を表わし、「サイズ」は、そのメールのサイズを表わす。「件名」は、そのメールの件名を表わし、「連絡」は、そのメールの送信者或いは必要な連絡先（メールウイルス連絡先テーブル参照）に連絡済みか否かを表わす。ここでは「連絡」で連絡済みの場合は「済」、連絡を行っていない場合は「未」で表わしている。

#### 【0027】

次に抑止条件設定テーブル118の構成を図8に示す。抑止条件設定テーブル118は、メールウイルス検出システム101上を送受信されるメールについて、メールウイルスに感染していると判断する基準を設定するテーブルであり、「送信者抑止」、「条件1」、「サイズ抑止」、「条件2」、「件名抑止」、「検出連絡」の6項目で構成される。

#### 【0028】

「送信者抑止」は、メールウイルス情報テーブル116にある「送信者」からのメールを抑止するか否かを表わし、「サイズ抑止」は、メールウイルス情報テーブル116にある「サイズ」と同じサイズのメールを抑止するか否かを表わし、「件名抑止」は、メールウイルス情報テーブル116にある「件名」と同じ件名のメールを抑止するか否かを表わす。ここでは「yes」となっている項目について同一のメールはメールウイルスに感染していると判断している。

#### 【0029】

「サイズ抑止」のみを「yes」にしていれば、同一サイズのメールは全て送信を抑止する。

#### 【0030】

「条件1」、「条件2」は、「送信者抑止」、「サイズ抑止」、「件名抑止」のどれをAND条件、あるいはOR条件で組み合わせて抑止するかを設定する項目であり、例えば「送信者抑止」と「件名抑止」の二つを「yes」、「条件1」を「and」にしておけば、送信者が同一かつ同一サイズのメールの送信を抑止する。

#### 【0031】

これにより、メールウイルスの認定は、最初にメールウイルス検出用アドレス

を判定し、メールウイルスに感染したメールがメールウイルス情報テーブル 116 に登録された後は上記二つのテーブルを利用して、件名、サイズ等の組み合わせでメールウイルスと認定することが可能になる。

【0032】

図 2 を用いて、メールウイルス検出システム 101 のメイン処理の具体的な動作を説明する。

【0033】

ステップ 201 でメールウイルス検出システム 101 が処理終了コマンドを受け付けたときは、処理を終了する。

【0034】

終了依頼がない時は次のステップへ進む。

【0035】

ステップ 202 でメールを受信したとき、アドレス判定処理 203（詳細は後述）を行う。

【0036】

メールを受信しないときは、メールが来るまで待つ。

【0037】

アドレス判定処理 203 の後、ステップ 204 でメールウイルス検出用アドレスを検出したことを示すメールウイルス情報テーブル 116 に「連絡」が「未」のデータがあり、かつ抑止条件設定テーブル 118 の「検出連絡」が「yes」であるものがあるかの比較判断を行う。

【0038】

条件を満足すればステップ 205 のウイルス連絡処理（詳細は後述）へ進む。

【0039】

条件を満足しなければステップ 206 のメール抑止処理（詳細は後述）へ進む。

【0040】

ステップ 205 のウイルス連絡処理を行なった後、ステップ 206 のメール抑

止処理へ進む。

【 0 0 4 1 】

ステップ 2 0 6 のメール抑止処理を終えるとメールウイルス検出システム 1 0 1 のメイン処理を終了する。

【 0 0 4 2 】

メールウイルス用アドレステーブル 1 1 7 の構成を図 6 で説明する。

【 0 0 4 3 】

メールウイルス用アドレステーブル 1 1 7 は LAN エリアにある各メールシステムクライアントに設定してあるメールウイルス検出用アドレスを、メールウイルス検出システムに登録するためのテーブルであり、メールウイルス検出用アドレスである「メールウイルス用アドレス」の項目だけから構成される。

【 0 0 4 4 】

次に、図 3 を用いてアドレス判定処理の具体例を説明する。

【 0 0 4 5 】

ステップ 3 0 1 でメールウイルス用アドレステーブル 1 1 7 に設定しているメールウイルス検出用アドレスである「メールウイルス用アドレス」宛てメールを受信したか否かを比較判断する。

【 0 0 4 6 】

条件を満足するときは、ステップ 3 0 2 で受信したメールの情報(「受信日時」、「送信者」、「サイズ」、「件名」)をメールウイルス情報テーブル 1 1 6 に登録し、連絡を「未」とする。

【 0 0 4 7 】

これにより、メールウイルス用アドレステーブル上の「メールウイルス用アドレス」に登録されていないメールウイルスに感染したメールでも、メールウイルス情報テーブル 1 1 6 に登録されている「送信者」、「サイズ」、或いは「件名」が同じメールならば、ステップ 2 0 4 で検出できるようになる。

【 0 0 4 8 】

条件を満足しないときには、処理を終了する。

【 0 0 4 9 】

メールウイルス連絡先テーブル120の構成を図10に示す。メールウイルス連絡先テーブル120は、メールウイルスに感染したメールを検出したときに連絡するための連絡先メールアドレスを登録するものであり、「連絡先アドレス」、「連絡レベル」、「備考」の3項目で構成される。

## 【0050】

「連絡先アドレス」は連絡先メールアドレスを表わし、「連絡レベル」は次に述べる連絡レベルテーブル119の「連絡レベル」を表わし、「備考」は具体的な連絡先の役割を表わしており、「system manager」か、メールウイルスに感染したメールの「送信者」か等を記録している。

## 【0051】

次に連絡レベルテーブル119の構成を図9に示す。連絡レベルテーブル119は、メールウイルスに感染したメールに関するログ、およびその期間とウイルスメールの圧縮を添付するレベルを登録するものであり、「連絡レベル」、「メールウイルス情報」、「ログ抽出対象ユーザ」、「ログ抽出対象履歴期間」、「ウイルスメール圧縮添付」の5項目で構成される。

## 【0052】

「連絡レベル」は、メールウイルスの情報（受信日時、送信者、サイズ、件名）とメールの送受信に関するログ、およびその抽出期間と抽出対象ユーザ、ウイルスメールの圧縮を添付するかの組み合わせのレベルを表わし、「メールウイルス情報」は、メールウイルス情報テーブル116に格納された情報を送信するときに「yes」、しない時は「no」で表わし、「ログ抽出対象ユーザ」は、ログを抽出する対象ユーザを表わし、ここでは「all」なら全ユーザ、「mailsendself」ならば、メールウイルス情報テーブル116の「送信者」を意味する。「ログ抽出対象履歴期間」は、ログを抽出する対象履歴の日数であり、ここでは「5day」なら5日分、「3day」なら3日分としている。「ウイルスメール圧縮添付」は、メールウイルスに感染したメールを圧縮して添付するか否かを表わしており、ここでは「yes」ならば添付し、「no」ならば添付しないとしている。

## 【0053】

次に、図4及び図5を用いてメールウイルス連絡処理の具体例を説明する。

【0054】

ステップ401で、メールウイルス連絡先テーブル120に登録してある「連絡先アドレス」を宛先とするメールウイルスの検出を連絡するメールひな型をそれぞれ設定する。

【0055】

ここでは、送信者宛てメールの内容に、『あなたの送信したメールは、ウイルスと見なされました。送信されません。』という内容を設定する。system manager、system manager (private)、system 2nd manager宛てのメールの内容には、『メールウイルスを検出しました。メールウイルス情報(受信日時、送信者、サイズ、件名)、全ユーザについて抽出した5日分のメール送受信ログ、該当するメールを圧縮添付します。』という内容を設定する。

【0056】

次にステップ402で、用意したメールひな型の宛先(メールウイルス連絡先テーブル120の「連絡先アドレス」)の「連絡レベル」に対応する連絡レベルテーブル119の「メールウイルス情報」が‘yes’であるか否かを比較判断する。

【0057】

条件を満足すれば、ステップ403でメールウイルス情報の連絡が‘未’のデータの受信日時、送信者、サイズ、件名をメールひな型に追加する。

【0058】

条件を満足しなければ、ステップ403をスキップする。

【0059】

次にステップ404で、用意したメールひな型の宛先(メールウイルス連絡先テーブル120の「連絡先アドレス」)の「連絡レベル」に対応する連絡レベルテーブル119の「ログ抽出対象ユーザ」が‘all’であるか否かを比較判断する。

【0060】

条件を満足すれば、ステップ405でメールの送受信を記録しているログファイルより、連絡レベルテーブル119にて対応する「連絡レベル」のログ抽出対象期間分の過去のログを抽出し、メールひな型に追加する。

【0061】

これにより、何日前からメールウイルスに感染したかを直ぐにログから調べることができるので、迅速な対応が可能になる。

【0062】

条件を満足しなければ、ステップ405をスキップする。

【0063】

次にステップ406で用意したメールひな型の宛先(メールウイルス連絡先テーブル120の「連絡先アドレス」)の「連絡レベル」に対応する連絡レベルテーブル119の「ログ抽出対象ユーザ」が‘mailsendself’であるか否かを比較判断する。

【0064】

条件を満足すれば、ステップ407でメールの送受信を記録しているログファイルより、連絡レベルテーブル119にて対応する「連絡レベル」のログ抽出対象期間分の過去のログを抽出し、かつメールウイルス情報テーブル116の「連絡」が‘未’のデータの「送信者」に関わるログを抽出し、メールひな型に追加する。

【0065】

‘mailsendself’の場合は、メールウイルス情報テーブル116の「送信者」宛にメールウイルスに感染したことを知らせ、迅速な対応を取らせるためである。

【0066】

条件を満足しなければ、ステップ407をスキップする。

【0067】

次にステップ408で用意したメールひな型の宛先(メールウイルス連絡先テーブル120の「連絡先アドレス」)の「連絡レベル」に対応する連絡レベルテーブル119の「ウイルスメール圧縮添付」が‘yes’であるか否かを比較判



断する。

【0068】

条件を満足すれば、ステップ409で受信したメールを圧縮し、メールひな型に添付する。

【0069】

条件を満足しなければ、ステップ409をスキップする。

【0070】

次にステップ410で、用意したメールひな型の全てについて処理したか否かを比較判断する。

【0071】

条件を満足すれば、ステップ411で用意したメールひな型を送信する。

【0072】

ここでは、メールの送信だけを説明しているが、必要に応じて自動でメール管理者への携帯電話連絡を行なう処理を追加してもよい。

【0073】

条件を満足しなければ、ステップ402へジャンプする。

【0074】

最後にステップ412でメールウイルス情報テーブル116の「連絡」が「未」のものを「済」にする処理を行い、処理を終了する。

【0075】

最後に、図12を用いてメール抑止処理の具体例を説明する。

【0076】

ステップ501で、メールウイルス情報テーブル116より「送信者」、「サイズ」、「件名」を読み取り、抑止条件設定テーブル118より、「送信者抑止」、「条件1」、「サイズ抑止」、「条件2」、「件名抑止」を読み取り、メールの送信抑止条件を作成する。

【0077】

次にステップ502で、受信したメールが、送信抑止条件に当てはまるか否かを比較判断する。

【 0 0 7 8 】

条件を満足すれば、ステップ 5 0 3 で受信したメールを送信しないで処理を終了する。

【 0 0 7 9 】

条件を満足しなければ、ステップ 5 0 4 で受信したメールを送信し、処理を終了する。

【 0 0 8 0 】

【発明の効果】

以上説明したように、本発明をメールシステムに備えることで、メールウイルスが LAN 内に入ってきた場合に、メールウイルスがメールウイルス検出用アドレスに送信した時点ですぐにメールウイルスを検出することができる。

【 0 0 8 1 】

そして、それ以降、メールウイルスに感染した可能性のあるメールの送信を設定に応じて自動的に抑止することが可能となる。また、メールウイルスの情報、関連するメール送受信ログ、メールウイルス自身の送信を複数のメールアドレスに対し、個別に必要な情報のみを連絡することができるようになる。

【 0 0 8 2 】

以上のことより、未知のメールウイルスであっても、早期に発見し、更にメールウイルスの蔓延を自動的に抑止し、影響範囲の調査、メールウイルスの調査を容易とすることが可能となる。

【図面の簡単な説明】

【図1】

メールウイルス検出システムの全体像を示す図。

【図2】

メールウイルス検出システムのメインフローチャート。

【図3】

アドレス判定処理のフローチャート。

【図4】

メールウイルス連絡処理のフローチャート。

【図 5】

メール抑止処理のフローチャート（その 1）。

【図 6】

メール抑止処理のフローチャート（その 2）。

【図 7】

メールウイルス情報テーブルを示す図。

【図 8】

抑止条件設定テーブルを示す図。

【図 9】

連絡レベルテーブルを示す図。

【図 10】

メールウイルス連絡先テーブルを示す図。

【図 11】

メールヘッダーを示す図。

【図 12】

メール抑止処理のフローチャート。

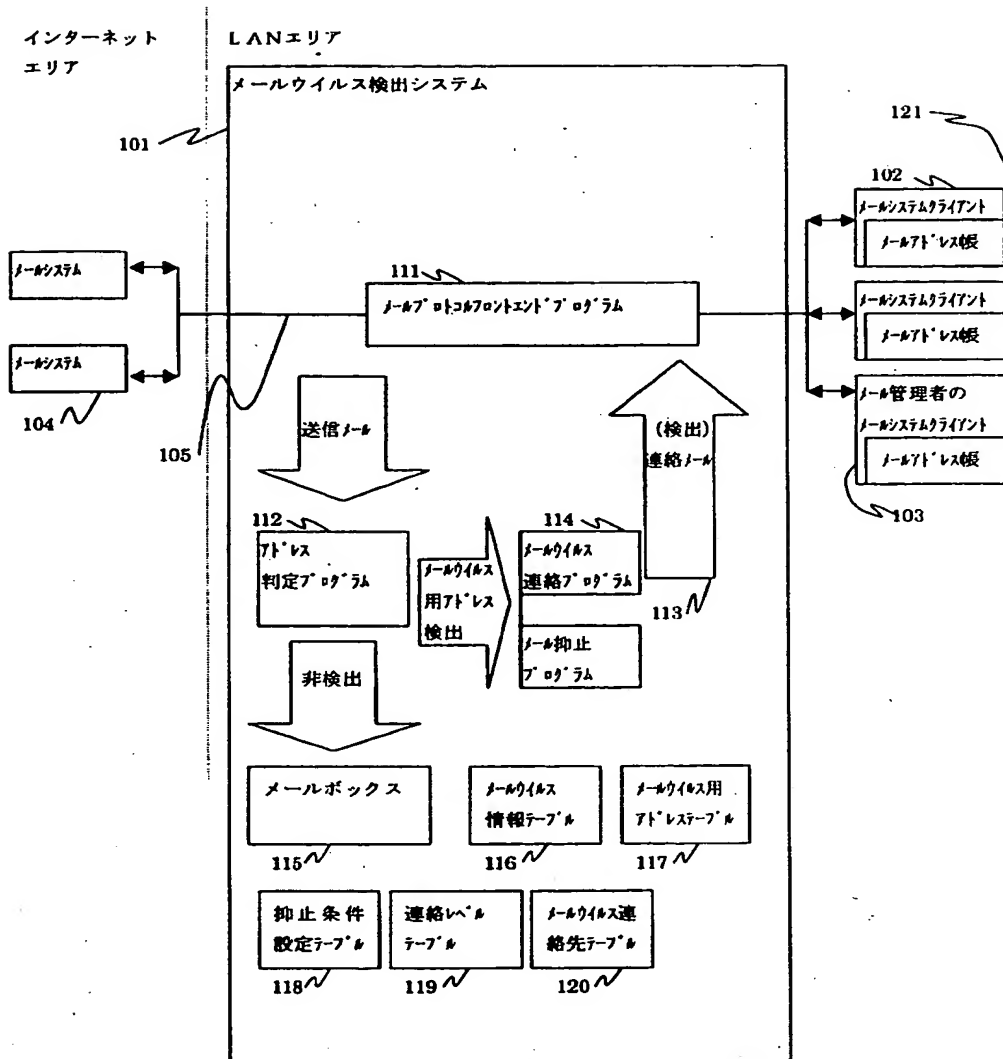
【符号の説明】

- 101 メールウイルス検出システム
- 102 メールシステムクライアント
- 103 メール管理者のメールシステムクライアント
- 104 インターネット上のメールシステム
- 105 ネットワーク

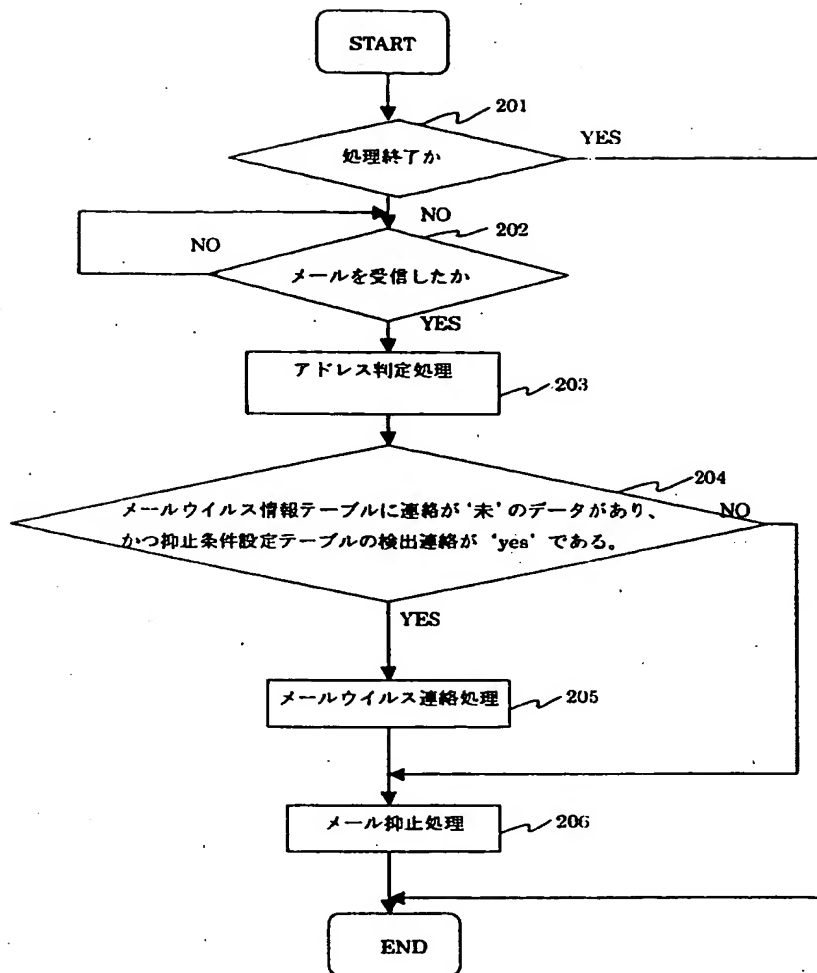
【書類名】

図面

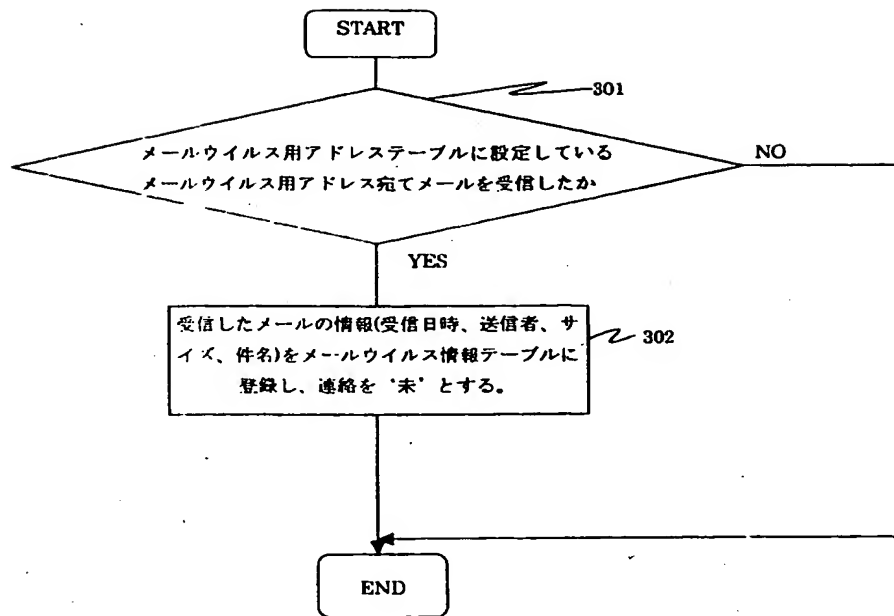
【図1】



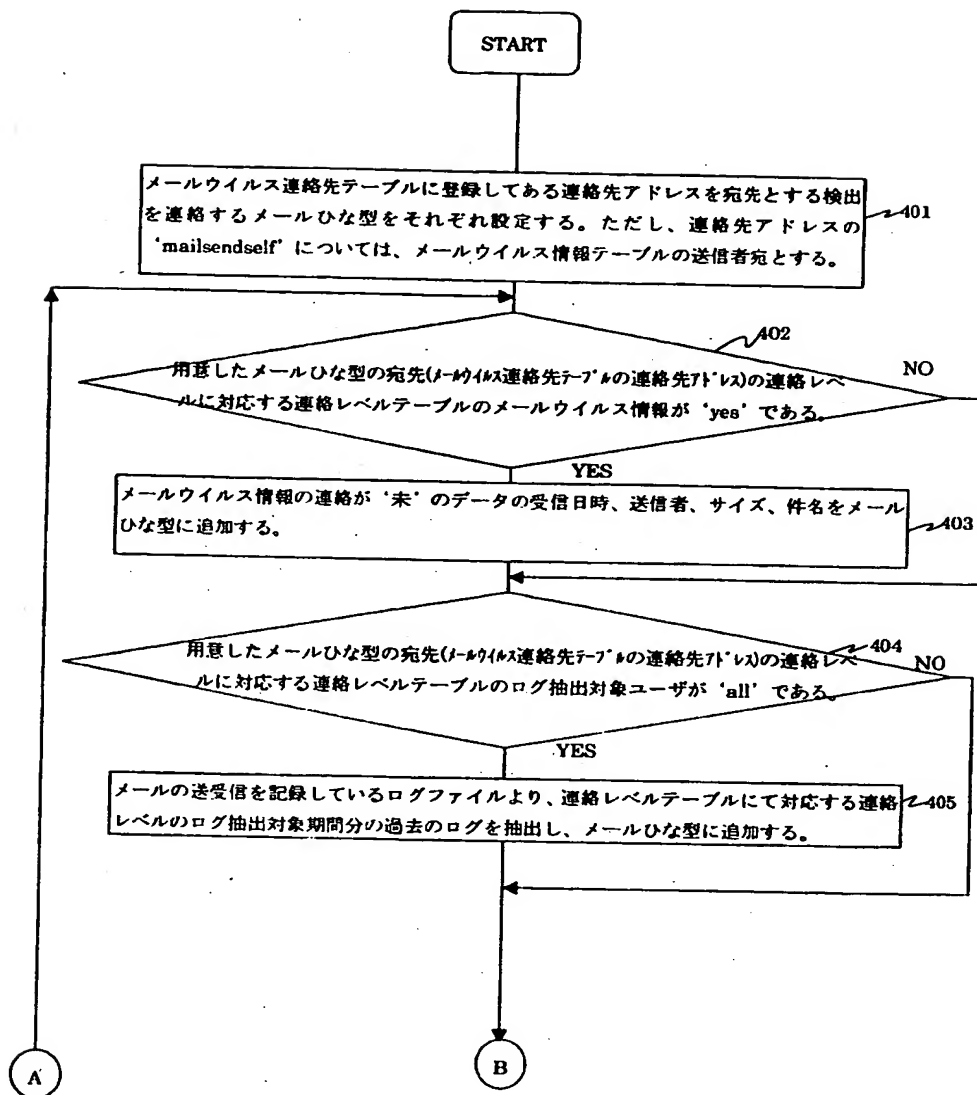
【図 2】



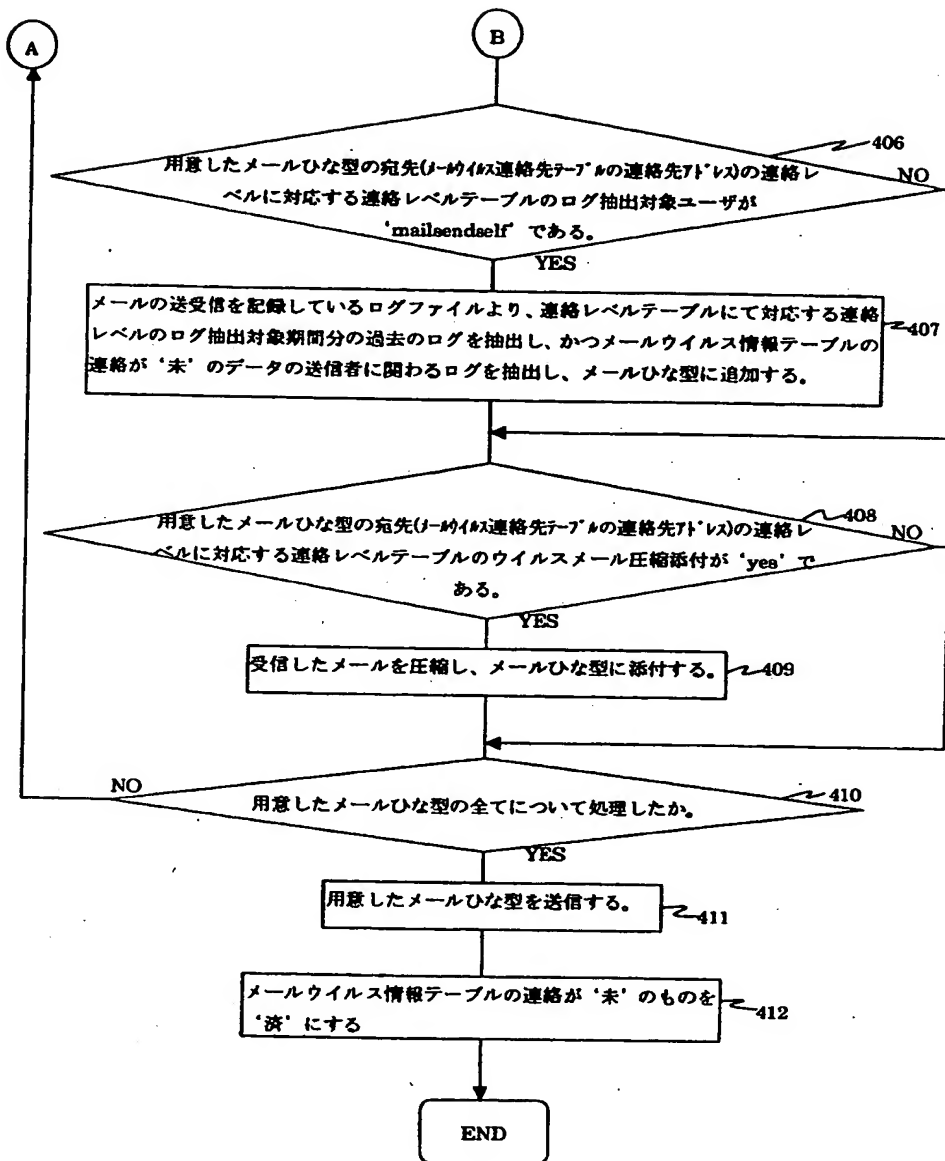
【図 3】



【図 4】



【図5】





【図6】

メールウイルス用アドレス
aaaaaaaaa@fss.co.jp
abcdefghi@fss.co.jp
viry@fss.co.jp

【図7】

受信日時	送信者	サイズ	件名	連絡
MMDDhhmmss	abc@fss.co.jp	1776	‘大切なお知らせ’	‘済’
MMDDhhmmss	def@fss.co.jp	1789	‘業務連絡’	‘未’

【図8】

送信者抑止	条件1	サイズ抑止	条件2	件名抑止	検出連絡
‘Yes’	‘or’	‘no’	‘or’	‘no’	‘yes’

【図 9】

連絡レベル	メールウイルス 情報	ログ抽出 対象ユーザ	ログ抽出 対象履歴期間	ウイルスメール圧縮添付
1	'yes'	'all'	'5day'	'yes'
2	'yes'	'all'	'5day'	'no'
3	'Yes'	'mailsendself'	'3day'	'no'
4	'yes'			'no'

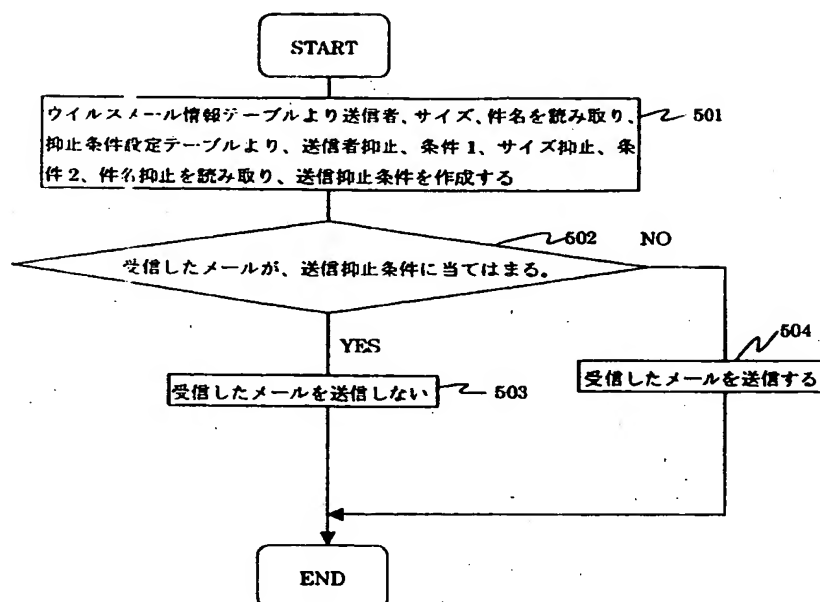
【図 10】

連絡先アドレス	連絡レベル	備考
'sys@fss.co.jp'	1	'system manager'
'taro@tukuba.ne.jp'	2	'system manager (private)'
'Sys2@fss.co.jp'	2	'system 2nd manager'
'mailsendself'	3	'送信者'

【図 1 1】

ヘッダー	内容
from :	送信元メールアドレス
to :	送信先メールアドレス
cc :	カーボンコピーの送信先メールアドレス
reply-to :	返信先メールアドレス
return-path :	エラーメールの送信先メールアドレス
.....	.....

【図 1 2】



【書類名】 要約書

【要約】

【課題】 未知のメールウイルスであっても早期に発見し、メールウイルスと思われるメールの送信を抑止し、メールウイルスの情報と発信者のメール送受信履歴を指定のメールアドレスに連絡すること。

【解決手段】 メールアドレスが通常は送信される予定のないメールウイルス検出アドレスへメールが送信されたか否かを判定するアドレス判定手段と、メールウイルス検出用アドレスへ送信されたメールと同型のメールの送信を抑止するメール抑止手段、メールウイルス検出用アドレスへメールが送信されたことを示すメールアドレス検出を連絡する必要がある相手に電子メールを送信するウイルス連絡手段を備えるメールウイルス検出システムによって上記課題を解決する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号

[000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社